

PCT

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
Bureau international



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PC

(51) Classification internationale des brevets ⁶ : G06F 1/00	A1	(11) Numéro de publication internationale: WO 97/46931 (43) Date de publication internationale: 11 décembre 1997 (11.12.97)
---	-----------	---

(21) Numéro de la demande internationale: PCT/FR97/00991

(22) Date de dépôt international: 4 juin 1997 (04.06.97)

(30) Données relatives à la priorité:
96/06923 5 juin 1996 (05.06.96) FR

(71) Déposant (pour tous les Etats désignés sauf US): CKD (S.A.)
[FR/FR]; 183, avenue Georges Clémenceau, F-92024 Nanterre Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (US seulement): DAPSANCE, Pierre
[FR/FR]; CKD (S.A.), 183, avenue Georges Clémenceau, F-92024 Nanterre Cedex (FR).

(74) Mandataire: BREESE-MAJEROWCIZ; 3, avenue de l'Opéra, F-75001 Paris (FR).

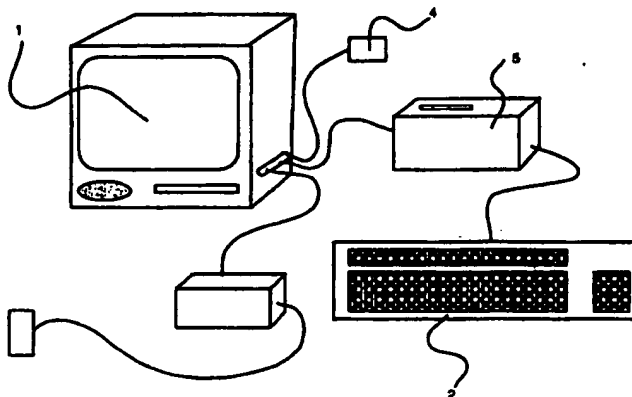
(81) Etats désignés: CA, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée

Avec rapport de recherche internationale.

(54) Title: DEVICE FOR ENSURING THE SAFETY OF COMPUTERISED TRANSACTIONS, IN PARTICULAR FOR ELECTRONIC PAYMENT

(54) Titre: DISPOSITIF POUR LA SECURISATION DE TRANSACTIONS INFORMATISEES, NOTAMMENT POUR LE PAIEMENT ELECTRONIQUE



(57) Abstract

The invention features a device for ensuring the safety of computerised transactions, in particular for electronic payment, consisting of a housing to be branched between the keyboard and the central processing unit (1), this housing containing an electronic circuit capable of verifying access authorisation and of modifying the connexion status between the keyboard and the central processing unit (1) between a direct connexion mode and a disconnected mode, the latter mode being activated during the access authorisation verification sequence.

DISPOSITIF POUR LA SECURISATION DE
TRANSACTIONS INFORMATISEES, NOTAMMENT POUR LE
PAIEMENT ELECTRONIQUE.

5 La présente invention concerne un dispositif
pour la sécurisation de transactions informatisées,
notamment pour le paiement électronique. Plus
particulièrement, elle concerne la sécurisation de
10 postes informatiques comprenant un terminal d'ordinateur
connecté au réseau téléphonique, ou plus généralement à
un réseau accessible par d'autres postes. On connaît
dans l'état de la technique de nombreuses solutions pour
la sécurisation de transactions informatisées. Certaines
15 mettent en oeuvre des cartes à mémoires, d'autres sont
basées sur des principes de cryptage, par exemple de
type R.S.A., impliquant l'usage de clés publiques et de
clés privées.

Toutes ces solutions ont en commun
l'inconvénient suivant : lorsque l'unité centrale est
20 reliée à un réseau, il n'est jamais possible de garantir
de manière absolue qu'un tiers ne puisse recueillir les
informations secrètes saisies par l'utilisateur
habilité. Ces informations secrètes sont par exemple le
code de la carte à mémoire ou la clé privée dans une
25 solution de cryptage.

Le but de la présente invention est de
remédier à cet inconvénient en proposant une solution
améliorant la sécurité par rapport à ce type de fraudes.

A cet effet, l'invention concerne plus
30 particulièrement un dispositif pour la sécurisation de
transactions informatisées, notamment pour le paiement
électronique, caractérisé en ce qu'il est formé par un
boîtier destiné à être branché entre le clavier et
l'unité centrale, ce boîtier contenant un circuit

encore une carte de personnalisation du poste de travail, de contrôle d'accès ou d'accréditation. Elle peut encore être une carte d'autorisation d'accès à un réseau informatique ou téléphonique, ou à un programme, fichier, zone de fichier ou espace de mémoire de l'ordinateur.

Selon un mode de réalisation avantageux, le lecteur de carte à mémoire comporte un moyen de détection de la présence de la carte assurant le passage de l'état de liaison entre le clavier et l'unité centrale en mode déconnecté, jusqu'à la fin du processus de vérification de l'autorisation d'accès. Selon une variante, le lecteur de carte à mémoire comporte un moyen de détection de la présence de la carte assurant le passage de l'état de liaison entre le clavier et l'unité centrale en mode direct en l'absence de carte à mémoire.

Selon un deuxième mode de réalisation, le circuit de vérification du boîtier calcule une clé d'autorisation en fonction d'informations transmises d'une part par l'unité centrale, et d'autre part délivrées par le clavier pendant le mode déconnecté. Ce mode de réalisation est particulièrement adapté en relation avec des systèmes de cryptage tel que R.S.A. ou asynchrone à clés publiques et privées ou DES.

Selon un mode de réalisation préféré, le circuit délivre à l'unité centrale, en mode déconnecté, des séquences de signaux de services telles que de démarrage ou de réinitialisation, ou d'interruption, lorsque le clavier délivre une séquence de signal correspondant. Ce mode de réalisation permet de conserver, même en mode déconnecté, la possibilité d'adresser à l'unité centrale des instructions fondamentales telles que la réinitialisation par

5 ailleurs relié au réseau téléphonique par l'intermédiaire d'un modem (modulateur-démodulateur) (3) ou d'une interface pour l'accès à un réseau numérique RNIS, par exemple NUMERIS (marque déposée). L'unité centrale (1) peut en outre être connectée à un boîtier (4) de raccordement à un réseau informatique sur lequel sont connectés l'ensemble des postes de travail ou un serveur local.

10 Le boîtier (5) est interposé entre l'unité centrale (1) et le clavier (2). Il est connecté d'une part au port clavier de l'unité centrale, et d'autre part sur la prise de raccordement du clavier.

15 Ce boîtier (5) ne modifie pas, au repos, la liaison entre le clavier et l'unité centrale (1). Il se comporte comme une liaison continue. Par contre, pendant les phases de vérification ou d'authentification, il crée une interruption physique entre le clavier et l'unité centrale de manière à ce qu'aucun signal électrique provenant du clavier (2) n'aboutisse à l'ordinateur. Pendant les phases de vérification ou d'authentification, le calculateur intégré dans le boîtier (5) exécute localement les procédures informatiques de certification et d'autorisation, en fonction des signaux qui proviennent de l'unité centrale (1) et/ou du clavier (2), sans que les informations traitées localement ou provenant du clavier (2) ne soient accessibles sur la sortie du boîtier (5).

20 La figure 2 représente le schéma de principe d'un dispositif selon l'invention. Le circuit reçoit des signaux Srcl provenant du clavier, des signaux Sruc provenant de l'unité centrale et délivre des signaux Secl vers le clavier et des signaux Seuc vers l'unité centrale. La liaison entre le clavier et l'unité centrale est interrompue physiquement et est rétablie

25

30

protocole de vérification. Lorsque le protocole arrive à l'étape de saisie d'informations confidentielles, le calculateur (10) commande le basculement du coupleur (11) dans le mode déconnecté. Les informations saisies à l'aide du clavier génère alors des signaux qui ne sont accessibles que par le calculateur. Le calculateur (10) peut délivrer sur la sortie Seuc des signaux différents, par exemple des "*" pour que l'unité centrale puisse commander l'affichage non pas des caractères saisis sur le clavier, mais des caractères ne permettant pas de reconstituer les informations saisies.

L'activation du protocole de vérification peut également être commandée par la détection d'une séquence particulière de signaux délivrés par l'unité centrale sur le port clavier. Il peut s'agir d'une séquence prédéterminée de signaux d'activation du bruiteur incorporé dans le clavier. Lorsque le calculateur détecte ladite séquence, il exécute un protocole de vérification stocké dans la mémoire (12) par exemple, ou encore dans l'ordinateur. Lorsque le protocole arrive à l'étape de saisie d'informations confidentielles, le calculateur (10) commande le basculement du coupleur (11) dans le mode déconnecté, comme dans le cas d'une certification à l'aide d'une carte.

L'invention est décrite dans ce qui précède à titre d'exemple non limitatif. L'Homme de Métier pourra réaliser différentes variantes sans pour autant sortir du cadre de l'invention. En particulier, il sera possible d'ajouter au boîtier une mémoire vive tampon ("BUFFER") assurant par ailleurs une déconnexion du clavier.

clavier et l'unité centrale (1) en mode direct en l'absence de carte à mémoire.

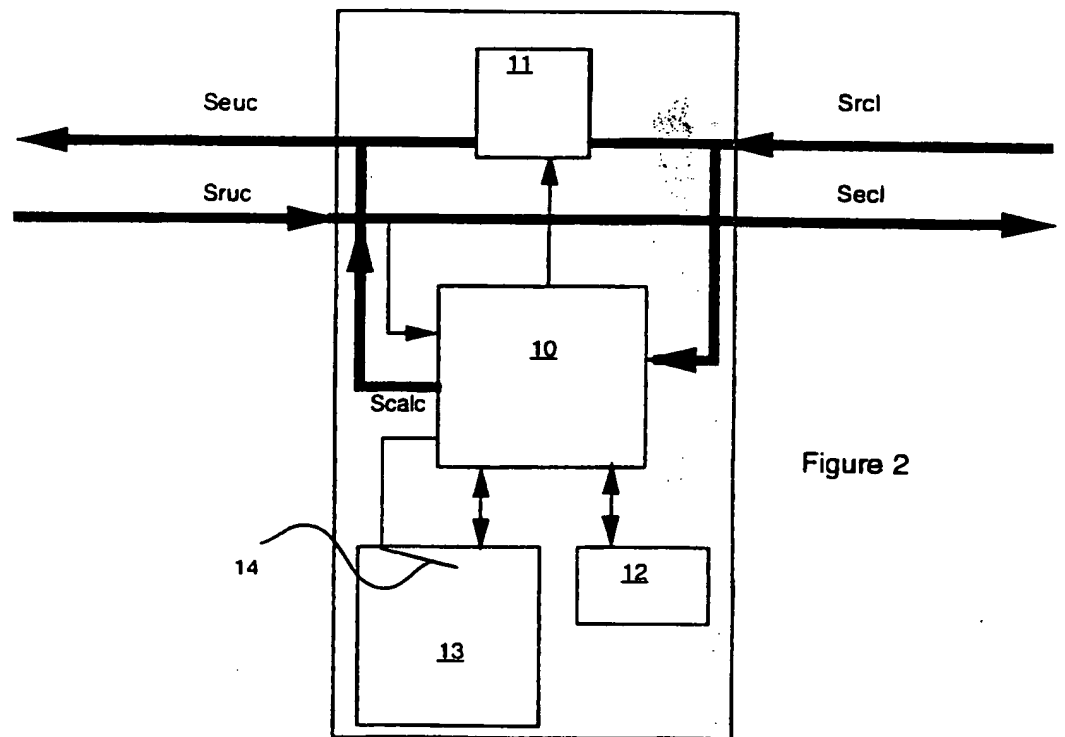
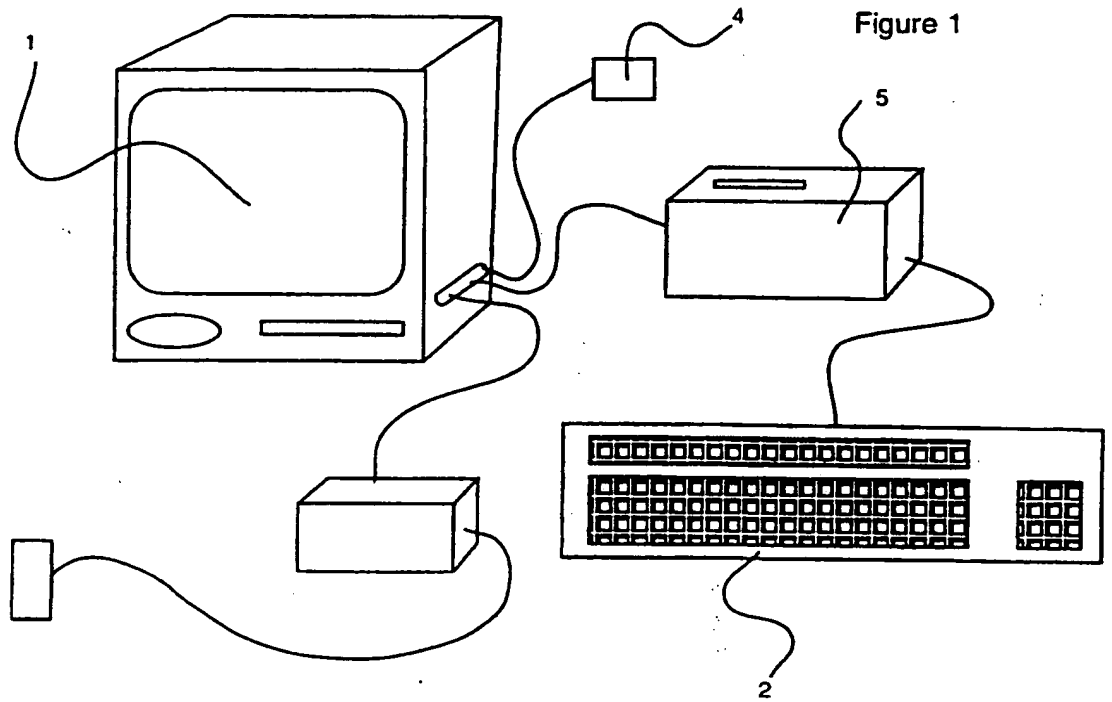
5 5 - Dispositif pour la sécurisation de transactions informatisées, notamment pour le paiement électronique, selon la revendication 1 caractérisé en ce que le circuit de vérification du boîtier calcule une clé d'autorisation en fonction d'informations transmises d'une part par l'unité centrale (1), et d'autre part délivrées par le clavier pendant le mode déconnecté.

10 6 - Dispositif pour la sécurisation de transactions informatisées, notamment pour le paiement électronique, selon l'une quelconque des revendications précédentes caractérisé en ce que le circuit délivre à l'une centrale, en mode déconnecté, des séquences de signaux de services telles que de démarrage ou de réinitialisation, ou d'interruption, lorsque le clavier délivre une séquence de signal correspondant.

20 7 - Dispositif pour la sécurisation de transactions informatisées, notamment pour le paiement électronique, selon l'une quelconque des revendications précédentes caractérisé en ce que le passage d'un état de liaison à l'autre état de la liaison entre le clavier et l'unité centrale (1) est commandé par un signal de service transmis par l'unité centrale (1) au clavier.

25 8 - Dispositif pour la sécurisation de transactions informatisées, notamment pour le paiement électronique, selon la revendication 7 caractérisé en ce que le passage d'un état de liaison à l'autre état de la liaison entre le clavier et l'unité centrale (1) est commandé par une séquence prédéterminée de signaux d'activation du bruiteur intégré dans le clavier.

30 9 - Dispositif pour la sécurisation de transactions informatisées, notamment pour le paiement électronique, selon l'une quelconque des revendications



INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/FR 97/00991

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0587375 A	16-03-94	IL 103062 A	04-08-96
		GB 2267986 A,B	22-12-93
		US 5406624 A	11-04-95

WO 9526085 A	28-09-95	US 5517569 A	14-05-96
		AU 2190295 A	09-10-95
		CA 2185697 A	28-09-95
		EP 0750812 A	02-01-97

NL 9101506 A	01-04-93	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. Internationale No

PCT/FR 97/00991

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0587375 A	16-03-94	IL 103062 A	04-08-96
		GB 2267986 A,B	22-12-93
		US 5406624 A	11-04-95
WO 9526085 A	28-09-95	US 5517569 A	14-05-96
		AU 2190295 A	09-10-95
		CA 2185697 A	28-09-95
		EP 0750812 A	02-01-97
NL 9101506 A	01-04-93	AUCUN	